STRATEGIC LATENCY AND WARNING:

PRIVATE SECTOR PERSPECTIVES ON CURRENT INTELLIGENCE CHALLENGES IN SCIENCE AND TECHNOLOGY

REPORT OF THE EXPERT ADVISORY PANEL WORKSHOP

LAWRENCE LIVERMORE
NATIONAL LABORATORY
January 8, 2016

CGSR
Center for Global Security Research

NATIONAL INTELLIGENCE UNIVERSITY
The Center of Academic Life for the Intelligence Community

“You can't lie about the future.”

— Edward Teller

Members of the Expert Advisory Panel on Strategic Latency and Warning

Project Managers:

Zachary Davis, Lawrence Livermore National Laboratory
Frank Gaç̄, Consultant for Lawrence Livermore National Laboratory
Ron Lehman, Lawrence Livermore National Laboratory
Michael Nacht, UC Berkeley

Expert Panel Members:

Paul Bracken, Yale University
Rudy Burger, Woodside Capitol Partners
James Canton, Global Futures Institute
David Chu, Institute for Defense Analysis
James Giordano, Georgetown University Medical Center
Toby Redshaw, Kevington Advisors

Rapporters:

Joey Ching, United States Air Force
Anthony Juarez, UC Berkeley

Observers and Participants:

Elshan Akhadov, Los Alamos National Laboratory
Ben Bahney, Lawrence Livermore National Laboratory
Thomas Campbell, National Intelligence Council
Nils Carlson, Lawrence Livermore National Laboratory
Ben Forster, FireEye Inc.
Pat Falcone, Lawrence Livermore National Laboratory
William Goldstein, Lawrence Livermore National Laboratory
Bruce Goodwin, Lawrence Livermore National Laboratory
Dimitri Kusnezov, U.S. Department of Energy
Jonathan Pearl, Lawrence Livermore National Laboratory
Joseph Price, U.S. Department of Defense
Steve Rottler, Sandia National Laboratory
Brian Shaw, National Intelligence University
Jennifer Snow, United States Air Force
Wes Spain, Lawrence Livermore National Laboratory
Robert Vince, Lawrence Livermore National Laboratory
Christopher Yerkes, National Intelligence University

Report written by Zachary Davis, Frank Gaç̄, and Michael Nacht with the assistance of Joey L. Ching.

Prepared by LLNL under Contract DE-AC52-07NA27344.

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

LLNL-TR-680815

Executive Summary

Lawrence Livermore National Laboratory and National Intelligence University convened a group of business experts to examine parallels between S&T competition in the marketplace and science and technology intelligence (S&TI). The experts identified the centrality of people — individuals and connected groups — to the successful development and application of latent S&T capabilities. People may indeed be more important to recognizing S&T potential than deep knowledge of any particular technology. This report explores the significance of this key insight for S&TI.

To more clearly understand trends, potential, and ultimate realization of emerging strategic threats from rapidly evolving, expanding, and globalized science and technology (S&T), one must more deeply study the people who are driving rapid S&T innovation. These entrepreneurial leaders shape the business environment for emerging S&T and assemble the components that are essential to the transformation of promising technical ideas to fully realized technological capabilities. An identifiable cadre of individuals from across the globe share certain characteristics, foremost of which is that they are typically driven by a ruthless vision to accomplishment. They are generally known to one another and are fierce competitors — and like-minded collaborators. They are central to the selection of "winning" S&T that ultimately is developed through commercialization. They make things happen and are driven to success.

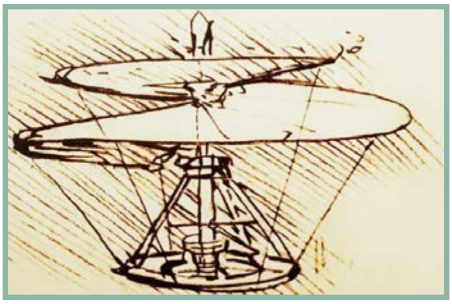
The hurdles of moving "good ideas" from concept to capability to operationally integrated practice are many and significant and absolutely require talented leadership to be overcome. Identifying, studying, and engaging that leadership cohort will provide unique, predictive insights into the S&T future they are creating. As an alternative to a focus on emergent technologies that may eventually pose a strategic threat to national security, focusing on the players who drive emerging technologies may well be a more predictive route to more clearly understand likely S&T futures and strategic threats. These people — through their investments, business acumen, and leadership — will determine the S&T future. A more complete understanding of their perspectives, their focus, their training and backgrounds, their investment of time and resources, and their global networks of peers promises greater insight into S&T futures than does attempts to monitor and track countless S&T developments that could — in theory — pose strategic national security threats.

Ill intent is not inherent to most of the technology of interest today, so the specific applications pursued by identifiable people must be considered and understood before appropriate national security responses can be developed. Strategic warning of genuine threats from S&T can only come from discovering actors who intend to use or develop a particular technology for malevolent purposes. It should be assumed that many/most of the technologies discussed today could be put to ill use if an actor had the intention. Therefore, identifying key international actors in the S&T community (individuals, companies, governments), defining their interests and goals, assessing enabling resource networks, and ultimately deriving specific intentions of these actors is essential to the delivery of credible strategic S&T threat warning. Establishing appropriate methods and capabilities to identifying, assessing, and divining intentions of these critical actors is an essential step toward an actionable strategic S&T threat warning capability.

Highlights from the Business Perspective on Emerging Technologies:

- Talented individuals pursuing a “clear ruthless vision” are the key factor in bringing S&T concepts from the laboratory to the marketplace — or battlefield;
- Successful technology investors outsource wherever possible and rarely participate in R&D efforts;
- Technology does not present a threat (commercially or for national security) unless it is embedded in a plan to use it for a specific purpose;
- Such plans must include doctrine, command and control and supporting systems that may themselves be identifiable and actionable;
- Cutting edge technology is often hard to develop and employ, whereas proven technologies are more readily adapted for commercial applications;
- Innovative business models that incorporate proven technology can be more disruptive than any technology alone.

Introduction:



Strategic Latency refers to the inherent potential of science and technology (S&T) to produce powerful tools capable of causing shifts in the balance of power. For the intelligence community (IC), knowledge and understanding of such tools are required to provide decision makers with strategic warning of emerging threats — and to alert them about opportunities to exploit technology trends.

Providing strategic warning of emerging S&T presents the IC with significant challenges. The challenges begin with information collection. As the IC attempts to keep track of the vast and rapidly evolving panoply of global S&T, it must also analyze S&T potential to threaten U.S. and global security. To provide strategic warning, the IC needs to understand specific S&T capabilities *and* the intent of an adversary to transform those capabilities into weapons that can be used against the U.S.. These insights are useful for policy makers and defense planners who are responsible for defending the nation.

This report on Strategic Latency builds on our previous studies of selected technologies and country profiles,[1] focusing specifically on the economic factors that determine which technologies successfully transition from scientific concept to commercial success. Commercial success is key to making new technologies widely available for constructive or malevolent purposes, even for governments. We want to know how latent potential can be exploited and turned into high-leverage weapons.

Rather than making extensive lists of technologies possessing latent potential that *could* be used for military purposes, and speculating how adversaries *might* employ them in the future, we gathered a group of business executives, management advisors, and economic experts to share their insights into the challenges of strategic latency and warning. The workshop showcased their thoughts and experiences selecting S&T investments, identifying failures, and calculating corporate and market risks. For example, we asked the experts:

- How do high-tech investors evaluate the commercial and competitive potential of emerging technologies?

- How does the private sector identify, cultivate, and react to emerging and disruptive technologies in the marketplace?

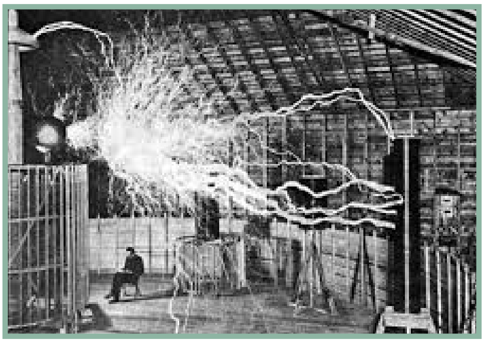
- What resources and strategies are required to transform a promising scientific concept into a market leader?

- How do investors recognize failures and disassociate with them?

This report captures the insights from the expert panel and relates them to the S&T warning challenges of the intelligence community.

[1] Zachary Davis, Ronald Lehman and Michael Nacht, *Strategic Latency and World Power: How Technology is Changing Our Concepts of Security* (Livermore: Lawrence Livermore National Laboratory, 2014)

Section 1. Defining Strategic Latency: What is Strategic about Science, Technology and Threat Warning?



Despite being among the most overused words in the modern English lexicon, we use "strategic" to denote extraordinarily consequential actions of a positive or negative nature. In the national security context, "strategic" implies widespread, long term effects for the nation state. "Strategic warning" describes the goal of alerting decision makers of impending strategic threats. "Strategic surprise" describes the failure to provide adequate warning, leading to "The sudden realization that one has been operating on the basis of an erroneous threat perception."[2] This arises from a failure to predict or anticipate an acute and immediate threat. Such threats must also have the following characteristics:

1. A discreet event or combined series of events, not a continuous process that arises from anticipated activity.
2. Significant national interests must be at stake to be "strategic" in nature.
3. Surprise arises from a failure to anticipate "immediate" threats, not potential threats. Potential threats are not actions but environments.
4. Must arise from actions posed by deliberate adversarial intent, not by accident or unintended consequences. These may lead to surprise, but is not a strategic surprise.
5. Intention arises from an identified adversary and strategic objectives.

> ***"Strategic: Relating to the identification of long-term or overall aims and interests and the means of achieving them."***
>
> — Oxford Dictionary

We use the term Strategic Latency to describe technologies that have significant potential to be transformed by a nation, group or individual for strategic effects. In the business world, this would include disruptive technologies, such as the Internet, that bring rapid and revolutionary change to the global marketplace. We asked our experts to apply their insights from the business world to the challenges facing Science and Technology Intelligence (S&TI), especially with respect to the analytic rigors of the strategic warning mission. While understanding that our primary focus is on analyzing foreign utilization of technology, (so-called "red" applications), our experts were eager

[2] Adapted from: Ariel Levite, *Intelligence and Strategic Surprise* (New York: Colombia Press, 1987)

to offer their perspectives on the related challenge of applying S&TI insights to inform U.S. development of S&T for defensive and offensive purposes. We address this aspect (for "blue" forces) in the final section.

Section 2. Insights from the Expert Panel on Strategic Latency

The expert panel collectively agreed that strategic latency is not limited to cutting edge technologies alone. Innovations in global business practices can be just as revolutionary in bringing latent technologies to market. Markets and business practices have as much to do with technology development as scientific research. Investors do not pay as much attention to "big science" conducted by large institutions (governments, labs, universities) as they do to smaller scale, applied research pursued by private entities. Thus, most technological "breakthroughs" will remain latent unless picked up by an investor. The panel members described innovative business models used to transform ideas into products and to keep companies competitive. All of the experts endorsed an "innovate or die" mindset, advising the IC to pay close attention to business developments if they want to track innovations in S&T.

Key attributes that enable businesses in the technology sector to compete successfully include the following:

- Focus on incremental improvements on proven technologies rather than big S&T breakthroughs;

- Speed to market — success in the tech sector depends on rapidly assembling the resources and organization needed to compete effectively;

- Risk is unavoidable — and the key to success;

- Invest in people first. Someone with a clear and persistent vision can succeed,regardless of the technology;

- Pay attention to IT. It's the key to speed and communication;

- Outsource wherever possible: In-house services are outmoded.

#Winning: Modern Business Practices Determine Winners and Losers in Technology

Panel members emphasized that in business, nothing is sacred. It is better to "cull the herd," accept losses, and move on, than to risk being trapped in an uncompetitive business model. There was broad consensus that S&T is evolving "at a speed and rate of acceleration that we have never seen before." Business has no choice but to "innovate or die." These realities complicate the job of the IC.

Panel members shared their perspectives on competitive practices that determine success or failure in technology markets. With access to expertise, resources and S&T knowledge fully globalized and available to all, success depends on putting together the

Emerging Technologies with Latent Potential

The latest emerging technology does not necessarily represent the greatest threat. History has shown that "old" or existing technologies can result in the unexpected. Thus, new, emerging technologies and old technologies both have the latent potential for surprise. Nonetheless, the following emerging technology areas merit monitoring for their latent potential:

- Revolutionary power, which embodies alternative energy production and advanced energy storage;
- Autonomous systems, which includes advanced robotics and the entire spectra of unmanned autonomous systems (UAS);
- Additive manufacturing, which spans the ever-advancing 3D printing and bio-printing realms, to the evolution of self-assembled structures or even nanoscale self-replicating machines;
- Information Technology (IT), including big data and analytics, but also quantum-enabled technology, social/business networking, and advanced communications;
- Biotechnology based upon synthetic "bio-building blocks," advanced genomics, and developments in neuroscience and neurotechnology;
- Advanced materials, which facilitate new sensing phenomena, enhanced properties and performance, or even new classes of structures and systems.

right combination of skills and means to achieve and maintain a competitive advantage. Outsourcing is essential for lean and agile operations: “In-house services are dead.” In addition to cost savings, outsourcing provides new perspectives that are increasingly needed to find efficiencies and identify opportunities. Outside expertise is also valuable in sharpening internal debates that are essential for progress. Companies that pay too much attention to perfecting their own technology risk being caught flat footed. Many technology companies outsource the development of the very technologies they seek to sell.

Regarding S&T expertise, one panel member quipped that “smart grows on trees.” Companies can easily find world class talent on any technical topic and contract for any needed services. The same is true for management and support staff. Peer to peer lending and electronic currency/banking is remaking business finance. Cool technology and good ideas are everywhere. The bigger challenge is to combine the suite of necessary skills and services to pursue a clear objective. However, the dynamism of the market dooms even the most effective business model to limited longevity. Nothing lasts.

The panel highlighted the importance of top shelf IT support as a key ingredient for success. Too often considered a backwater, IT support has become a critical element for agile decision making and information security. The most innovative business models depend on IT systems to be a force multiplier which should not be relegated to secondary status. The participants noted the contrast with government IT systems and discussed possible implications of antiquated IT systems for the S&TI mission. How might the IC enhance its understanding of the role of IT in advancing foreign S&T developments?

> ***“Smart grows on trees.”***
>
> — Panel Member

Several panel members referenced the cautionary tale of Kodak, which was a global market leader that had multiple opportunities to adapt, yet failed. Despite being ideally positioned to exploit the revolution in digital imagery technology, Kodak made a fatal decision to cling to its investments in wet chemistry film processing. Staying in their comfort zone and doing what they knew best proved to be their downfall. Technology company leaders now understand the “innovate or die” nature of the marketplace and act accordingly. One possible implication for the IC is the global connections that all successful technology companies must maintain to remain competitive. Newly established supply chains may present opportunities for the IC to track innovative technologies, especially big systems such as space and large scale computers.

While governments can still control sensitive research in closed facilities, most of the innovation that is driving S&T is conducted by the private sector using global supply networks. This includes critical technologies such as cyber, robotics, biosciences, and even space technology. For investors, there is a strong preference of software over hardware, which requires more physical and cumbersome components. It is essential to understand the business model that governs the proliferation of these technologies.

Predicting the Emergence of New Technologies is Not the Primary Objective.

The IC puts great emphasis on forecasting, or predicting S&T development, especially by potential adversaries and competitors. From a business perspective, however, forecasting has significant limitations and plays only a supporting role in decision making. Attempting to accurately predict which technologies will prove viable and worthy of investment overlooks older "latent" technologies that may be rediscovered to have innovative and disruptive power. Several panel members cited Uber as an example of a disruptive business model that hacks existing technologies to redefine the market. ***Efforts to predict which technologies will become market-ready should guard against the risk of missing the context in which new ideas can be disruptive and revolutionary.***

Forecasting is a valuable tool that is used by technology companies to support business decisions. Such tools prove most useful in scoping potential R&D breakthrough areas and analyzing market trends — both of which are important for analyzing potential threats. Panel members cited crowdsourcing and big data analysis as useful, but said they seek a variety of perspectives from multiple analytic services rather than associate with any particular foresight provider. They recommended that the IC not rely on its own internal forecasting capabilities and instead make use of a variety of private analytic services using innovative methods such as crowdsourcing and multi-source big data.

Some panel members took the view that prediction and forecasting is an inherently reactive approach to future planning, and thus limits opportunities to innovate and compete. A noted futurist and author/advisor stressed the importance of being "future ready" to create opportunities rather than harvest those that are assessed to be ripe for exploitation. He advised the intelligence community to take a proactive approach to the emerging technology "mountaintops" that will define the international environment. He urged us to define our needs and objectives proactively and chart a technology path to get there without waiting to analyze foreign progress. By the time we recognize that our adversaries are exploiting new technologies, it will be too late.

Shifting his emphasis to the related issue of U.S. (blue force) planning, he urged the IC to shape and define our desired future rather than passively watch what comes through the R&D pipeline. "Whoever claims the mountaintop will define the future, not those who predict and react."

The panel members applied this "mountaintop" logic to intelligence challenges in space, cyber, big data, robotics, and other technology areas. There was broad recognition that China has already begun its quest to dominate certain technological mountaintops, as evidenced by Beijing's aspirational five year plans to guide technology development.[3] The intelligence community should identify and pursue our own "mountaintops" or risk losing out to those who do. The panelists generally agreed that China is successfully exploiting strategic latency and that strategic warning should have been clearly communicated to policy makers with respect to China's S&T capabilities and intentions.

Several panel members warned against taking a linear perspective on technology innovation and relying on historical precedent to assess current S&T practices. New

[3] Tai Ming Cheung, "Strategic Latency with Chinese Characteristics: The Quest to Realize Its Strategic Potential in the 21st Century," in Strategic Latency and World Power: How Technology is Changing Our Concepts of Security (Livermore: Lawrence Livermore National Laboratory, 2014)

business models open new approaches that may not have identifiable precedents. A venture capital investor on the panel highlighted a "new narrative at work" in global business that makes it possible for competitors from very different backgrounds and circumstances to access technology and compete in new ways. More important than sophisticated scientific knowledge, business leaders rely on a "clear, ruthless vision" and then take the necessary steps to bring that vision to life. The alternative is to be washed away by the wave of rapid innovation. ***The lesson for the IC is to be nimble and pay attention to a broad spectrum of S&T innovators of diverse backgrounds.***

Old and Reliable Outsmarts New and Improved

In his keynote address to the expert group, the president of a major defense think tank observed that some of the most consequential technology is not changing as fast as some might think. While there is intense competition to bring new commercial products to market, much of the recent technology innovation has been concentrated in consumer electronics. Overall, automobiles, aircraft, and weapon systems remain largely consistent with historical patterns. Change is incremental. Radical innovations are rarely adopted. Panelists cited IEDs, the use of social media by terrorist organizations, and SCUD missiles as examples of old technologies being used effectively by our adversaries. One panel member made the point that most "new" technology is not new at all, but is re-purposed to be faster, smaller, and cheaper. "It's all out there for everyone to see."

> ***"The sun is new each day."***
>
> — Heraclitus

New applications of technology, embedded in innovative concepts of operation, may pose more serious threats than groundbreaking but unproven scientific discoveries. Too much emphasis on potential game changing, "bolt from the blue" S&T innovations could distract us from more subtle "frog in the pot" types of threats that use old technologies to attack our interests in new ways. A noted scholar of technology and business elaborated: "In most cases, it isn't the technology alone that matters, but a larger set of issues." ***Technology is one part of a broader equation of intentions and capabilities that combine to create threats.***

Certain technologies lend themselves more easily to the private sector emphasis on speed and innovation in business practices. One panel member, an expert in biotechnology, noted that neuroscience is a rapidly evolving domain in which important scientific progress is being achieved through relatively small scale efforts, relying on small research teams, widely available equipment, and with limited budgets. By employing top scientific talent and the most advanced methods, small-scale research laboratories are now capable of cutting edge breakthroughs that could have significant military applications. More dangerous yet, the activities of these laboratories are difficult to detect or monitor.[4] Small companies, non-governmental organizations and even Do It Yourself (DIY) hobby groups are capable of very advanced experimentation and even production of potentially hazardous agents. The group agreed that biotechnology and the businesses associated with it are evolving so quickly that it would be extremely difficult to provide strategic warning of specific emerging military applications.

Global norms of oversight, peer review, and human subject protection may not prevail. Our biotechnology expert urged the group to consider the growing potential for hostile, illicit, or irresponsible groups and individuals to engage in experimentation that could have very widespread consequences. In his view, the U.S. is currently "outgunned" in neuroscience, which is receiving growing attention from state and non-state actors.

The IC needs to pay closer attention to the requirements that adversaries are seeking to satisfy with their acquisition of specific technology. Members of the group noted that recent reorganizations within the IC were designed to bring analysts and collectors into closer collaboration and that this would be consistent with the panel's recommendation for increased integration of S&T capability analysis with the collection of specific threat actor information.

"Technology doesn't kill people; People kill people."

— Panel Member

Cultural factors often influence how countries and companies approach their S&T goals. In this regard, strategic latency is no different than any other topic of political, economic and military analysis. Our panel did not offer insights into the cultural, historic, and geo-political influences that shape the R&D environment in particular foreign countries. Our previous report and other studies have addressed this point.[5] The panel did, however, highlight the importance of the environmental factors that define the motivations for pursuing particular technologies. As one panel member put it, "Context is worth 80 IQ points." Such factors shape technology development from the laboratory through the process of development to the production, marketing and deployment of technology-based products.

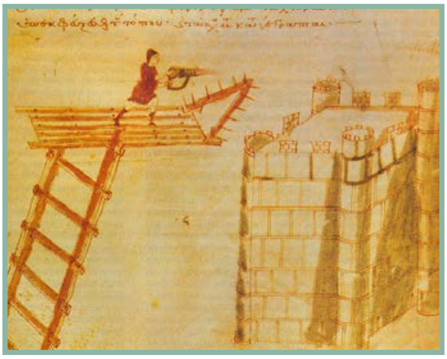
Understanding foreign technology development starts with an appreciation of the national and cultural norms, ethics, and common practices that shape their strategy and tactics. One panelist noted that profit is often not a primary motivator for innovation, as shown by the Islamic States' (ISIL's) employment of social media as a recruitment tool and its incorporation of white Toyota pick up trucks for rapid mobility to support military aggression. Even Silicon Valley start-ups are often motivated to bring revolutionary change to markets and society. Understanding what the people behind the technology want is more important than understanding the technology itself.

Not all technology-seeking countries and groups share U.S. values, and some may not respect current norms of war and politics. Rules governing intellectual property, respect for borders, prohibitions against targeting civilians, and treaties to constrain the proliferation of weapons of mass destruction may not prevent rule-breakers from using S&T innovation to pursue their objectives. The panel members identified non-state

[4] James Giordano, editor, Neurotechnology in National Security and Defense (Boco Raton: CRC Press, Taylor and Francis, 2015)
[5] Strategic Latency and World Power, op cit.; S&T Strategies of Six Countries (Washington DC: National Academies Press, 2013).

actors as likely suspects to challenge established international standards. As one panel member observed, “The boundary between sympathizers and actors has become foggy,” making it difficult to determine how effective propaganda, radicalization, and simple instruction can affect seemingly harmless technologies. For example, it is hard to predict if common household items are acquired for practical use, or will be turned into bombs. A rising generation of disenfranchised, angry youth can just as easily be mobilized, either for constructive purposes or for war. Our biologist, who is also a noted bioethicist, cited access to advanced biological sciences as a credible means by which small groups who do not respect established norms of behavior could challenge the most powerful actors in the current world order. ***The panel advised the U.S. government to engage broadly with cutting edge S&T internationally to understand trends and motivations as well as track possible bad actors.***

Section 3. Threats Require a Combination of Intent and Capability



We asked our panel to consider three case studies where adversarial intent has been joined with technological capabilities and speculate on technology trends that warrant strategic warning because they could present threats to U.S. security.[6] Our breakout groups did not possess subject matter expertise on the country they were assigned, to asses but were instructed to project the trajectory of technologies that pose the most significant threats to U.S. security.

China: Poster Child for Strategic Latency

China has made the development of critical technologies a top priority. The list of technologies that China is pursuing through state-sponsored efforts includes many with direct military applications. China’s strategy for managing U.S. military power, especially U.S. military presence and political/military influence in the Asia-Pacific region, uses technology to offset U.S. advantages in conventional and nuclear power. High on Beijing’s list of desired technologies are biotech, materials research, robotics and manufacturing, and anything that will extend their reach further into space. China is also able to utilize its world class computing capabilities for commercial, scientific, and military purposes.

The group acknowledged China’s longstanding practice of acquiring foreign technology through licit and illicit means to jumpstart its own research programs and boost its competitive advantage. They judged this ongoing effort to be largely successful. China’s leadership sees technology as essential for stimulating economic growth and managing its growing population. China takes full advantage of its participation in the international economy and its relations with other countries to acquire technology. Efforts to stop China from poaching U.S. technology thus far have been ineffective.

> ***“Know thy self, know thy enemy. A thousand battles, a thousand victories.”***
>
> — Sun Tzu

[6] Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Armed Services Committee, James R. Clapper, Director of National Intelligence, February 26, 2015.

China is seeking particular technologies to address identified needs, many of which have been outlined in official publications. Members of the group suggested that previous investments in cyber and space technologies were now paying off, supporting elements of China's asymmetric military strategy. They warned, however, against overemphasis on cutting edge technologies in lieu of less sophisticated approaches. For example, their island building campaign in the South China Sea relies on basic dredging and landfill techniques for strategic effect. There was consensus that the IC should have communicated strategic warning about China's cyber and space activities and should be on the lookout for similar advancements.

North Korea: Making the Most of What They've Got

Although our expert panel members possess little knowledge about North Korea, much less its business culture, the breakout group assessed that the DPRK has developed a unique ability to acquire and utilize key defense technologies. North Korea leverages its relationships, particularly with China, to gain access to the technologies it needs for its defense. Building on its former relations with the Soviet Union, Pyongyang has reverse engineered a variety of nuclear and missile technologies to arm itself with an increasingly powerful strategic arsenal. North Korea then markets those defense technologies to its global clients through its illicit global proliferation networks and applies lessons from working with them to improve operational performance.

The group acknowledged North Korea's ability to creatively use global finance, transportation, and business networks to buy and sell a wide range of legitimate, grey, and black market commodities. The unique DPRK business model relies on key trusted individuals to operate its international networks. They concluded that it would be a mistake to underestimate North Korea's ability to acquire, adapt and employ advanced technologies and market them through its crude but effective illicit business model.

Russia: Technology Constrained but Aggressive Policies Unchecked

Technology investors have essentially abandoned Russia, according to our expert panel members. Putin's aggressive international behavior has foreclosed on what remained of the struggling technology investment community. Corruption and the absence of legal protections had already stifled tech investment and driven entrepreneurs to emigrate. State-sponsored technology centers never flourished, and Western investors judged the risks to be unacceptably high. Russia, therefore, will be forced to rely on established technologies and use state-sponsorship to apply them to defense needs. The Russian economy, however, will probably face long-term difficulties that will constrain the exploitation of Russia's tradition of world class S&T. The group did not expect such economic and political constraints to lessen Russia's ability to threaten U.S. interests, but agreed that Moscow will face tough choices if it is forced to expend scarce resources to modernize its military capabilities.

> ***"The Present only has a being in Nature; things Past have a being in the Memory only, but things to come have no being at all; the Future but a fiction of the mind."***
>
> — Thomas Hobbes, Leviathan

The group noted that new global business models open the possibility that Russia will be able to outsource some of its technological needs, as it has in the cyber world. Finally, Moscow may rely on its relationships with China and other technologically advancing nations to get access to cutting edge goods and services and should be expected to use espionage to overcome limitations of its indigenous technological innovation capabilities.

Section 4. Implications of Private Sector Insights for Science & Technology Intelligence

Technology is not a threat unless it is employed by an adversary for malevolent purposes. Greater understanding of the intent to acquire and use technology for military purposes is a precondition for strategic warning. As our keynote speaker described the analytic challenge: "By understanding the rational requirements of a threat actor, the range of technology necessary to fulfill objectives will be narrowed and thus become tractable for analysis." Once we know what our competitor/adversary is trying to achieve, a range of analytic tools and methods are available to characterize the severity and timing of technology threats. The panel members advocated for rigorous scientific reality testing of emerging and unproven S&T to determine threat potential, but advised the IC to interact with the global S&T business community to keep pace with commercial developments.

> ***"You can design and create, and build the most wonderful place in the world. But it takes people to make the dream a reality."***
>
> — Walt Disney

Our expert panel members provided insider insights into the inner workings of global high tech markets and offered ideas about how the IC could navigate modern business practices to improve S&TI. They highlighted biotech as an area that lends itself to extremely rapid and difficult to monitor developments. Innovations in financing, outsourcing, simulation and modeling using high performance computing, rapid prototyping, and global connectivity combine to accelerate the transition of scientific ideas to the market. However, the panel was united in the view that some of the most disruptive effects for the private sector come from new ways to use old technology. They advised against focusing exclusively on the most novel and new S&T concepts and to carefully consider how existing technology might be incorporated into new operational concepts. The group cited China as an example of a competitor who is using commercially available technology to compete economically and militarily.

Although most private sector experiences are not easily transferrable to the IC or the USG, understanding current international business practices is essential for tracking global S&T. Even if we are not "future ready" ourselves, we must maintain situational awareness of those who are exploiting strategic latency for commercial purposes. They are often the gatekeepers for those who seek technology for aggressive military applications.

The distinct challenges posed to the U.S. national security enterprise by the Cold War stand-off with the USSR and the on-going "Global War on Terror" have been summarized in a way that may be useful in thinking about the latent S&T threat. The Cold War threat (i.e. the USSR) was "easy to find but hard to kill," and the terrorist threat is "hard to find but easy to kill." In that sense, potential threats posed by global S&T are easy to imagine, difficult to analyze, and (perhaps) uniquely challenging to "kill." Largely a result of the fact that most of the developing and emerging technologies are only a threat if and when some actor employs them to do harm to U.S. national interests, it is virtually impossible to predict and warn of a specific threat — particularly at the strategic level — until it is manifest. Our Cold War adversary gave us clear intent along with relatively easily identifiable threat infrastructure but was a formidable foe not easily defeated. Terrorists with clear intent to do harm offer a much reduced set of threat "signatures," hamstringing otherwise straightforward defeat options. S&T by itself has no inherent "intent" but provides significant capability for myriad threats to those who do have such intent.

> ***"Well the future for me is already a thing of the past."***
>
> — Bob Dylan

Ill intent is not inherent to most of the technology of interest today, so the applications actually pursued by people must be considered and understood before appropriate national security responses can be developed. Strategic warning of genuine threats from S&T can only come from discovering actors who intend to use or develop a particular technology to do harm. Therefore, identifying key international actors in the S&T community (individuals, companies, governments), defining their interests and goals, assessing enabling resource networks, and ultimately deriving specific intentions of these actors is essential to the delivery of credible strategic S&T threat warning. Establishing appropriate methods and capabilities to identify, assess, and divine intentions of these critical actors is an essential step toward an actionable strategic S&T threat warning capability.

Section 5. What Happens after Strategic Warning?

What happens if the IC succeeds in delivering strategic warning of an S&T threat? Many of the same insights that inform the IC's ability to provide strategic warning can be applied to current efforts aimed at improving USG access to advanced S&T.[7] The application of S&T knowledge to U.S. defense needs is referred to as "blue force" requirements. Decision makers and defense planners can use strategic warning about red force capabilities to develop and implement response strategies. Those responses can cover the spectrum from political, economic and military options.

The expert advisory group offered important insights on ways the USG can exploit strategic latency to advance our own intelligence and military capabilities. Options include:

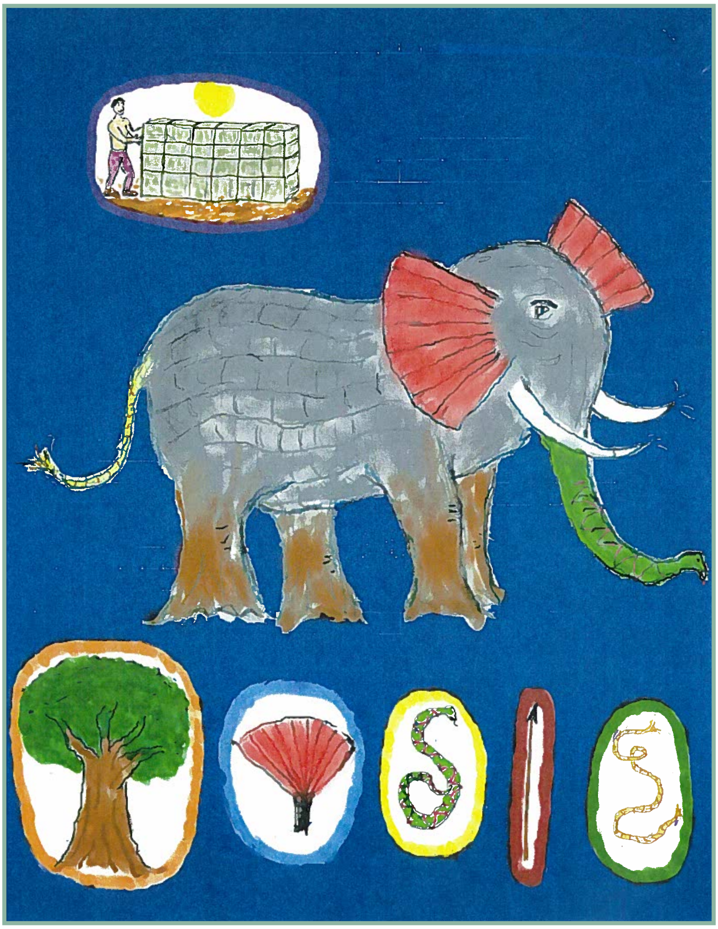
- Maintain a Skunk Works–type research capability to test novel S&T concepts and evaluate their potential applications to U.S. requirements;
- Develop strong relationships with private sector technology investors to keep pace with developments and identify promising S&T investments;
- Hire consultants and advisors from the venture capital community to help navigate global business operations;
- Accept more risk to invest with global business leaders rather than wait for market-proven commodities.

[7] Remarks by Secretary Carter at the Drell Lecture, Cemex Auditorium, Stanford Graduate School of Business, Stanford

Efforts along these lines are underway. Outreach efforts to Silicon Valley in the form of the CIA's In-Q-Tel,[8] the DOD's Defense Innovation Unit Experimental (DIUX),[9] and SOCOM's Thunderdome,[10] seek to accelerate USG access to cutting edge technologies. Moreover, the National Laboratories engage in applied research to identify and develop potentially useful emerging technologies. The expert panel members expressed concern that these government-led efforts are still too encumbered by bureaucratic limitations and lack the flexibility to exploit truly cutting edge technologies on behalf of the USG.

Final Thoughts: Follow the People

The job of providing strategic warning about emerging S&T threats is getting harder, but is still achievable. While the scope and pace of scientific discovery makes it increasingly difficult to track all the possible ways that technology *could* be used for malevolent purposes, people are still the primary actors. Thus, focusing on the individuals, businesses, sponsors, and investors who are bringing technologies into the marketplace presents a formidable but manageable challenge.



A matter of perspective

[8] https://www.iqt.org
[9] http://www.diux.mil
[10] http://www.tbo.com/list/military-news/altman/socom-looks-to-enhance-interactions-with-industry-academia-20150518/